Personal Data Protection Act

Passed 12 June 1996

(RT1 I 1996, 48, 944),

entered into force on 19 July 1996,

amended by the following Acts:

19.06.2002 entered into force 01.09.2002 - RT I 2002, 63, 387;

19.06.2002 entered into force 01.08.2002 - RT I 2002, 61, 375;

09.05.2001 entered into force 01.01.2002 - RT I 2001, 50, 283;

13.12.2000 entered into force 08.01.2001 - RT I 2000, 104, 685;

15.11.2000 entered into force 01.01.2001 - RT I 2000, 92, 597;

30.05.2000 entered into force 01.08.2000 - RT I 2000, 50, 317;

15.12.98 entered into force 03.01.99 - RT I 1998, 111, 1833;

17.06.98 entered into force 10.07.98 - RT I 1998, 59, 941.

Chapter 1. General Provisions ➦

§ 1. Purpose of Act

The purpose of this Act is protection of the fundamental rights and freedoms of persons with regard to processing of personal data in accordance with the right of persons to freely obtain information disseminated for public use.

§ 1.1. Application of Administrative Procedure Act

The provisions of the Administrative Procedure Act (RT I 2001, 58, 354; 2002, 53, 336)

apply to administrative proceedings prescribed in this Act, taking account of the specifications provided for in this Act.

(19.06.2002 entered into force 01.08.2002 - RT I 2002, 61, 375)

§ 2. Scope of application of Act

(1) This Act applies to:

1) the wholly or partly automatic processing of personal data;

2) the manual processing of personal data if the personal data used are taken from a structured set of personal data or intended to be included in a structured set of personal data.

(2) This Act does not apply to:

1) processing of personal data collected by natural persons themselves for personal use;

2) processing of personal data containing state secrets.

§ 3. Protection of personal data

(1) In order to ensure protection of personal data, chief processors and authorised processors have the duty to:

1) process personal data for the purposes and under the conditions specified in this Act;

2) comply with the personal data processing requirements and protection measures pursuant to the procedure provided for in this Act;

3) register processing of sensitive personal data pursuant to this Act.

(2) Protection of personal data is also ensured by a person's right, pursuant to the procedure provided for in this Act, to:

1) consent to processing of personal data relating to him or her;

2) receive information concerning processing of personal data relating to him or her;

3) prohibit processing of personal data relating to him or her.

§ 4. Personal data

(1) Personal data are any information relating to an identified natural person or a natural person identifiable directly or indirectly by reference to the person's physical, mental, psychological, economic, cultural or social characteristics, relations and associations.

(2) For the purposes of this Act, personal data are either sensitive or non-sensitive personal data.

(3) Sensitive personal data are:

1) data revealing political opinions, or religious or philosophical beliefs, except data relating to being a member of legal persons in private law registered pursuant to procedure provided by law;

(17.06.98 entered into force 10.07.98 - RT I 1998, 59, 941; 15.11.2000 entered into force 01.01.2001 - RT I 2000, 92, 597)

2) data revealing ethnic or racial origin;

3) data relating to state of health, genetic information or sexual life;

(13.12.2000 entered into force 08.01.2001 - RT I 2000, 104, 685)

4) (Repealed - 15.11.2000 entered into force 01.01.2001 - RT I 2000, 92, 597)

5) information collected in criminal proceedings or in other proceedings to ascertain an offence before a public court session or before a judgment is made in a matter concerning an offence, or if this is necessary in order to protect public morality or the family and private life of persons, or where the interests of a minor, a victim, a witness or justice so require.

(15.11.2000 entered into force 01.01.2001 - RT I 2000, 92, 597)

(4) The list of sensitive personal data may be supplemented by an Act regulating the corresponding area.

(5) Collected statistical data relating to a natural person are not personal data if it is not possible to identify the person relating to whom the data are collected.

§ 5. Processing of personal data

Processing of personal data is the collection, recording, organisation, storage, alteration, consultation, retrieval, use, disclosure, combination, closure, erasure or destruction of personal data or several of the aforementioned operations, regardless of the manner in which the operations are carried out or the means used.

§ 6. Chief processor and authorised processor

(1) A chief processor is a natural or legal person, or a state or local government agency who processes personal data or on whose order personal data are processed and who, pursuant to this Act, other Acts or legislation established on the basis thereof, is competent to determine:

1) the purposes of processing of personal data;

2) the categories of personal data to be processed;

3) the procedure for and manner of processing personal data;

4) permission for disclosure of personal data to third persons.

(2) An authorised processor is a natural or legal person, or a state or local government agency who processes personal data on order from the chief processor.

§ 7. Third person

(1) A third person is a natural or legal person, or a state or local government agency who is not:

1) an authorised processor;

2) a person whose personal data are processed;

3) a person subordinate to a chief processor or authorised processor who processes personal data.

(2) A third person who processes personal data disclosed to the third person by a chief processor is a chief processor pursuant to subsection 6 (1) of this Act, and the third person is required to comply with the requirements of this Act, other Acts and legislation established on the basis thereof in processing personal data.

Chapter 2. Permission for Processing Personal Data ➦

§ 8. Permission for processing non-sensitive personal data

(1) Processing of non-sensitive personal data is permitted without the consent of the person if the purpose of processing is:

1) performance of a contract entered into with the person or performance of work carried out on an order placed by the person;

2) protection of the person's life, health or freedom;

3) performance of obligations prescribed by law or international agreements;

4) performance of a task in the public interest which is assigned by law or legislation established on the basis thereof to a chief processor or a third person to whom the data are disclosed;

5) consideration of general interests, the legitimate interests of a chief processor or the legitimate interests of a third person to whom the data are disclosed, unless the interests of the person are more significant.

(2) Disclosure to third persons of non-sensitive personal data processed for the purposes specified in subsection (1) of this section is permitted if the processing thereof, including use by a third person, is carried out for such specified purposes. If processing of non-sensitive personal data, including use thereof by a third person, is not carried out for such specified purposes, disclosure of such data is only permitted with the consent of the person.

(3) Processing of personal data, including disclosure thereof to a third person, is permitted for purposes which are not specified in subsection (1) of this section if the person has given

consent therefor and the processing is not contrary to law or legislation established on the basis thereof.

§ 9. Permission for processing sensitive personal data

(1) Processing of sensitive personal data revealing political opinions or religious or other beliefs of an Estonian citizen or an alien residing in Estonia on the basis of a permanent residence permit, including disclosure thereof to a third person, is only permitted with the consent of the person. In other cases, processing of sensitive personal data revealing political opinions or religious or other beliefs of a person, including disclosure thereof to a third person, is permitted:

1) without the consent of the person if the processing is carried out for the performance of obligations prescribed by law;

2) with the consent of the person unless the processing is contrary to law or legislation established on the basis thereof.

(2) Processing of sensitive personal data revealing ethnic or racial origin, state of health, genetic information or sexual life is permitted without the consent of the person if the processing is carried out:

1) for performance of obligations prescribed by law;

2) for protection of the person's life, health or freedom;

3) for performance of a task in the public or general interest which is assigned by law to a chief processor or a third person to whom the data are disclosed.

(13.12.2000 entered into force 08.01.2001 - RT I 2000, 104, 685)

(3) Processing of personal data relating to criminal convictions, judicial punishments or a criminal proceeding is permitted without the consent of the person if the processing is carried out:

1) for performance of obligations prescribed by law;

2) for performance of a task in the public or general interest which is assigned by law to a chief processor or a third person to whom the data are disclosed.

(4) In other cases, processing of sensitive personal data specified in subsections (2) and (3) of this section is permitted if the person has given consent therefor and the processing is not contrary to law or legislation established on the basis thereof.

(5) More specific conditions for permitting processing of sensitive personal data shall be provided for in an Act regulating the corresponding area.

(6) Personal data shall be released in accordance with this Act and the Public Information Act, and pursuant to the procedure prescribed by other Acts if a special procedure for the release of a particular kind of personal data is provided therein.

(15.11.2000 entered into force 01.01.2001 - RT I 2000, 92, 597)

9.1. Permission for processing personal identification code

Processing of the personal identification code is permitted without the consent of the person if the purpose of processing is:

1) performance of an obligation prescribed by law or international agreements;

2) performance of a task in the public interest which is assigned by law or legislation established on the basis thereof to a chief processor or a third person to whom the data are transferred.

(30.05.2000 entered into force 01.08.2000 - RT I 2000, 50, 317)

§ 10. Consent of person

(1) Consent of a person is an explicit expression of intention whereby the person permits processing of personal data relating to him or her after the person is informed of:

1) the purpose of and legal basis for processing of personal data;

2) the categories and source of personal data;

3) third persons or categories thereof to whom disclosure of the personal data is permitted;

4) the list of personal data intended for public use;

5) the name and address of the chief processor or representative of the chief processor.

(2) Consent is valid with respect to a specific processing operation, must be given freely and may be withdrawn by the person at any time. Withdrawal of consent has no retroactive effect.

Chapter 3. Personal Data Processing Requirements and Protection Measures ➦

§ 11. Personal data processing requirements

A chief processor and authorised processor are required to process personal data only for the purposes and under the conditions precisely specified and permitted in this Act and to ensure that:

1) the categories of personal data are compatible with the purposes of processing and are not excessive in relation to the needs for achievement of these purposes;

2) personal data which are not necessary for achievement of the purposes are erased or closed;

3) personal data are accurate, and if necessary for achievement of the purposes, kept up to date;

4) incomplete and inaccurate personal data are closed, and necessary measures are immediately taken for amendment or rectification thereof;

5) inaccurate data are stored with a notation concerning their period of use together with accurate data;

6) personal data which are contested on the basis of accuracy are closed until the accuracy of the data is verified or the accurate data are determined.

§ 12. Organisational and technical measures to protect personal data

(1) In view of the categories of personal data to be processed, chief processors and authorised processors are required to take organisational and technical measures to protect personal data against:

1) accidental or intentional tampering;

2) accidental loss and intentional destruction;

3) unauthorised organisation, disclosure or other processing.

(2) In the automatic processing of personal data, chief processors and authorised processors are required to:

1) prevent access of unauthorised persons to equipment used for processing personal data (access control);

2) prevent the unauthorised reading, copying, alteration or removal of data carriers (data carrier use control);

3) prevent the unauthorised recording of personal data and alteration or erasure of recorded personal data (recording control) and to ensure that it be subsequently possible to determine when, by whom and which personal data were altered;

4) prevent the unauthorised use of a data processing system for the transmission of personal data by data communication equipment (data communication control);

5) ensure that every user of a data processing system only has access to personal data permitted to be processed by him or her (access control);

6) store information concerning disclosure of personal data regarding when, to whom, by whom and which personal data were disclosed (disclosure control);

7) ensure that it be subsequently possible to determine when, by whom and which personal data were input into the data processing system (input control);

8) ensure that unauthorised reading, copying, alteration or erasure is not carried out in the transmission of personal data by data communication equipment and in the transportation of data carriers (transport control);

9) organise the work of enterprises, agencies and organisations in a manner that allows compliance with special data protection requirements (organisational control)

(3) Chief processors and authorised processors are required to familiarise persons subordinate to them with legislation regulating processing of personal data and, in the case of the automatic processing of personal data, arrange for the training of such persons.

§ 13. Requirements for selection of authorised processors

A chief processor is required to select as persons to fulfil orders placed such authorised processors who will ensure that organisational and technical measures are taken to protect personal data pursuant to § 12 of this Act.

§ 14. Requirements for contract entered into for processing of personal data

(1) In order to process personal data, a chief processor and authorised processor shall enter into a written contract which shall observe the requirements of this Act, other Acts and legislation established on the basis thereof.

(2) The contract shall provide that the authorised processor is required to:

1) process personal data only pursuant to the procedure, in the manner and under the conditions prescribed in the contract;

2) apply the prescribed technical and organisational measures to protect personal data;

3) enter into subcontracts only under the conditions permitted in the contract.

(3) The contract shall prescribe liability of the parties for non-performance of the contractual obligations.

(4) An authorised processor is prohibited from disclosing, outside of the contract, personal data processed for the performance of the contract to third persons, except if:

1) the chief processor has given written consent therefor;

2) the disclosure obligation is prescribed by law.

§ 15. Requirements for persons who process personal data

(1) Persons who process personal data as chief processors or authorised processors and persons subordinate to chief processors or authorised processors who process personal data are required to process and disclose such for the purposes and under the conditions specified in this Act.

(2) The persons specified in subsection (1) of this section are required to maintain the confidentiality of personal data which become known to them in the performance of their duties and which are not intended for public use, and business secrets even after performance of their duties relating to the processing, or after termination of their employment or service relationships.

§ 16. Documentation of processing personal data

(1) Chief processors are required to prepare, store at the site of processing and, in the cases prescribed in this Act, submit:

1) the main information concerning processing of personal data;

2) a list of equipment and means used in processing (in the automatic processing of personal data);

3) the organisational and technical measures taken to protect personal data.

(2) Copies of the documents specified in subsection (1) of this section are kept with the authorised processor, who is required to submit them in the cases prescribed in this Act.

(3) The main information concerning processing of personal data must include the following information:

1) the names, location or residence of the chief processor and authorised processor;

2) the purposes of and legal basis for processing of personal data;

3) the categories of personal data;

4) the categories of persons whose data are processed;

5) the sources of personal data;

6) third persons or categories thereof to whom disclosure of the personal data is permitted;

7) the list of personal data intended for general use;

8) the conditions for closure and erasure of personal data;

9) the conditions for transfer of personal data to foreign states.

(4) Lists of equipment and means must include the following information:

1) the name, type, number and location of equipment used and the name of the producer of the equipment;

2) the name and licence number of software used and the name of the producer of the software;

3) the location of the software used and corresponding documents.

(5) Details of compliance with § 12 of this Act shall be provided in the organisational and technical measures to protect personal data.

(6) If personal data are processed by an authorised processor, the list of equipment and means and the organisational and technical measures to protect personal data may be prepared by the authorised processor.

(7) Amendments to the documents specified in subsection (1) of this section shall be made before the corresponding amendments are implemented in the processing of personal data.

Chapter 4. Registration of Processing Sensitive Personal Data ➦

§ 17. Registration requirement

(1) Chief processors are required to register processing of sensitive personal data with the data protection supervision authority.

(2) If a chief processor applies for an activity licence or a licence in an area of activity which involves the processing of sensitive personal data, the issuer of activity licences is required, before issuing the activity licence or licence, to obtain a document regarding registration of the processing of sensitive personal data from the data protection supervision authority.

(19.06.2002 entered into force 01.08.2002 - RT I 2002, 61, 375)

§ 18. Registration application

(1) A registration application shall be submitted at least one month before processing of sensitive personal data commences. A chief processor may submit a joint registration application for processing of sensitive personal data for several same or related purposes.

(2) A registration application shall set out the name and address of the chief processor and the name and address of the authorised processor, if any, and the following shall be appended thereto:

1) the main information concerning processing of sensitive personal data pursuant to subsection 16 (3) of this Act;

2) the organisational and technical measures to protect personal data pursuant to § 12 of this Act;

3) the names and personal identification codes of owners (stockholders) of the chief processor who is a legal person if the chief processor is not a state or local government agency.

§ 19. Decision on registration

(1) The data protection supervision authority shall within fifteen working days after the date of receipt of a registration application decide to register or refuse to register the processing and shall notify the chief processor or representative of the chief processor thereof.

(19.06.2002 entered into force 01.08.2002 - RT I 2002, 61, 375)

(2) The data protection supervision authority shall refuse to register processing of sensitive personal data if:

1) processing of sensitive personal data is contrary to this Act, other Acts or legislation established on the basis thereof;

2) the organisational and technical measures to protect personal data do not ensure compliance with the requirements provided for in § 12 of this Act;

3) the registration application and documents appended thereto do not include the information necessary for registration.

(3) If processing of sensitive personal data is particularly prejudicial to the rights and freedoms of a person, the data protection supervision authority is required to inspect preparations for processing of personal data on site. In such case, the term for notification of registration or refusal to register is extended by ten working days. As a result of inspection, the data protection supervision authority may give recommendations for application of supplementary organisational and technical measures to protect personal data.

§ 20. Notification of alteration or amendment of information

Chief processors are required to notify the data protection supervision authority of alteration or amendment of the information specified in subsection 18 (2) of this Act within fifteen working days before implementation of the corresponding alterations or amendments. The data protection supervision authority has the right to prohibit implementation of the corresponding alterations and amendments if these are not in accordance with this Act, other Acts or legislation established on the basis thereof.

Chapter 5. Rights of Persons ➦

§ 21. Person's right to receive information before collection of personal data

(1) If consent of a person is necessary for processing of personal data, a chief processor or representative of the chief processor shall, before collection of personal data, inform the person pursuant to subsection 10 (1) of this Act.

(2) A chief processor or representative of the chief processor is required to inform the person of the alteration or amendment of the information specified in subsection 10 (1) of this Act not later than fifteen working days before implementation of the corresponding alterations or amendments. The person has the right to prohibit implementation of the specified alterations or amendments.

§ 22. Person's right to receive information and personal data relating to him or her in processing of personal data

(1) At the request of a person, a chief processor shall inform the person of:

1) the existence or absence of personal data relating to him or her;

2) the purpose of and legal basis for processing of personal data;

3) the categories and source of personal data;

4) third persons or categories thereof to whom disclosure of the personal data is permitted;

5) the name and address of the chief processor or representative of the chief processor.

(2) A person has the right to receive personal data relating to him or her from a chief processor.

(3) A person has the right to receive personal data relating to him or her from a chief processor once a year free of charge. Thereafter, the person has the right to receive personal data relating to him or her for a fee. The fee shall not exceed the expenses in connection with the provision of data.

(4) A chief processor is required to provide a person with information and the requested personal data or state the reasons for refusal to provide data or information pursuant to § 25 of this Act within fifteen working days after the date of receipt of an application.

(5) The obligations of the chief processor provided for in this section also extend to the authorised processor who maintains a database containing personal data.

(30.05.2000 entered into force 01.08.2000 - RT I 2000, 50, 317)

§ 23. Person's demand to rectify, close or erase personal data

(1) A person has the right to demand from a chief processor:

1) the rectification of inaccurate personal data;

2) the closure or erasure of personal data if the processing is contrary to this Act, other Acts or legislation established on the basis thereof.

(2) A chief processor is required to immediately inform third persons to whom personal data have been disclosed of the rectification of inaccurate personal data or the closure or erasure of personal data.

(3) A chief processor and third persons are required to satisfy a person's justified demand immediately unless otherwise provided by law.

(4) The obligations of the chief processor provided for in this section also extend to the authorised processor who maintains a database containing personal data.

(30.05.2000 entered into force 01.08.2000 - RT I 2000, 50, 317)

§ 24. Person's right to prohibit disclosure of personal data relating to him or her for public use

A person has the right to prohibit disclosure of personal data relating to him or her for public use unless this is contrary to this Act, other Acts or legislation established on the basis thereof.

§ 25. Exceptions to right to receive information and personal data

(1) A person's right to receive information before collection of personal data pursuant to § 21 of this Act and a person's right to receive information and personal data relating to him or her in the processing of personal data pursuant to § 22 of this Act are restricted if this may prejudice:

1) the rights and freedoms of other persons;

2) protection of the confidentiality of filiation of a child;

3) prevention of a criminal offence or apprehension of a criminal offender;

4) ascertainment of the truth in a criminal proceeding.

(2) A decision to refuse to provide data or information shall be made by a chief processor, who shall notify the person thereof.

(19.06.2002 entered into force 01.08.2002 - RT I 2002, 61, 375)

§ 26. Person's right of recourse to data protection supervision authority or court

A person has a right of recourse to the data protection supervision authority or a court if the person finds that his or her rights are violated or freedoms are restricted in the processing of personal data.

Chapter 6. Supervision over Processing of Personal Data ➦

§ 27. Supervision

The data protection supervision authority shall monitor observance of the requirements of this Act and legislation established on the basis thereof. The data protection supervision authority shall be the Data Protection Inspectorate.

(15.12.98 entered into force 03.01.99 - RT I 1998, 111, 1833)

§ 28. Requirements for head of data protection supervision authority

(1) A person who has completed higher education in law may work as the head of the data protection supervision authority.

(2) A person who has been released or removed from any position or office requiring higher education in law due to unsuitability for continued work shall not be the head of the data protection supervision authority.

(3) The head of the data protection supervision authority shall not hold any other remunerative position or office during his or her term of office.

(4) The head of the data protection supervision authority is, in the performance of his or her functions, independent and shall act pursuant to this Act, other Acts and legislation established on the basis thereof.

§ 29. Maintenance of confidentiality of personal data

Employees of the data protection supervision authority are required to maintain business secrets and the confidentiality of personal data which become known to them in the performance of their duties, even after termination of their service relationships with the state.

§ 30. Rights and duties of data protection supervision authority

(1) The data protection supervision authority has the right to:

1) monitor compliance with the personal data processing requirements provided by this Act, other Acts and legislation established on the basis thereof;

2) register processing of sensitive personal data pursuant to the procedure provided for in this Act;

3) resolve petitions and challenges filed with the personal data protection supervision authority with regard to the processing of personal data;

(19.06.2002 entered into force 01.08.2002 - RT I 2002, 61, 375)

4) issue precepts pursuant to the procedure provided for in § 31 of this Act;

5) demand relevant documents and other necessary information from persons;

6) provide persons with information and arrange for training in the processing and protection of personal data;

(2) The rights set out in subsection (1) of this section are also duties of the data protection supervision authority.

(3) Competent officials of the data protection supervision authority have the right of unhindered access to inspect the offices of persons who process personal data.

(4) Chief processors and authorised processors are required to provide competent officials of the data protection supervision authority with statements and provide them with access to documents and equipment, including recorded data, and to software used for data processing if this is necessary for inspection of processing of personal data.

§ 31. Precepts of data protection supervision authority

(1) An official of the data protection supervision authority has the right to issue the following precepts to a chief processor and authorised processor:

(19.06.2002 entered into force 01.08.2002 - RT I 2002, 61, 375)

1) to terminate violation of the personal data processing requirements by a specified date;

2) to take supplementary organisational and technical measures to protect personal data by a specified date;

3) to register processing of sensitive personal data by a specified date.

(09.05.2001 entered into force 01.01.2002 - RT I 2001, 50, 283)

(2) Upon failure to comply with a precept specified in subsection (1) of this section, the data protection supervision authority may impose a penalty payment pursuant to the procedure provided for in the Substitutive Enforcement and Penalty Payment Act.

(09.05.2001 entered into force 01.01.2002 - RT I 2001, 50, 283)

(3) The upper limit of penalty payment specified in subsection (2) of this section is 10 000 kroons.

(09.05.2001 entered into force 01.01.2002 - RT I 2001, 50, 283)

§ 32. (Repealed - 19.06.2002 entered into force 01.09.2002 - RT I 2002, 63, 387)

Chapter 7. Liability ➦

(19.06.2002 entered into force 01.09.2002 - RT I 2002, 63, 387)

§ 33. Violation of requirements of Personal Data Protection Act

(1) Violation of the obligation to register the processing of sensitive personal data, violation of the requirements regarding measures to protect personal data or violation of other requirements for the processing of personal data is punishable by a fine of up to 300 fine units.

(2) The same act, if committed by a legal person, is punishable by a fine of up to 50 000 kroons.

(3) The provisions of the General Part of the Penal Code (RT I 2001, 61, 364; 2002, 44, 284; 56, 350) and the Code of Misdemeanour Procedure (RT I 2002, 50, 313) apply to the misdemeanours provided for in this section.

(4) The Data Protection Inspectorate is the extra-judicial body which conducts proceedings in matters of misdemeanours provided for in this section.

(19.06.2002 entered into force 01.09.2002 - RT I 2002, 63, 387)

§ 34. (Repealed - 19.06.2002 entered into force 01.09.2002 - RT I 2002, 63, 387)

1 RT = Riigi Teataja = State Gazette